WEST Search History

DATE: Monday, July 28, 2003

Set Name side by side	Query	Hit Count	Set Name result set
	DB=USPT; THES=ASSIGNEE; PLUR=YES; OP=OR		
L6	L5 and ((telephone or phone) with (record or data or report$))	1	L6
L5	5901228.pn.	1	L5
L4	L3 and l2	2	L4
L3	((705/30 |705/34)!.CCLS.)	400	L3
L2	(((telephone or phone) with (record or data or report$)) and ((log$ or record$) same ((host$ adj (network$ or computer or station)))) and (authori$ near2 user) and @ad<=19980116)	98	L2
	DB=USPT,PGPB,JPAB,EPAB,DWPI,TDBD; THES=ASSIGNEE; PLUR=YES; OP=OR		
L1	(((telephone or phone) with (record or data or report$)) and ((log$ or record$) same ((host$ adj (network$ or computer or station)))) and @pd<=19980116)	550	L1

END OF SEARCH HISTORY

End of Result Set

Generate Collection | Print

L4: Entry 2 of 2 File: USPT May 4, 1999

US-PAT-NO: 5901228
DOCUMENT-IDENTIFIER: US 5901228 A

TITLE: Commercial online backup service that provides transparent extended storage to remote customers over telecommunications links

DATE-ISSUED: May 4, 1999

INVENTOR-INFORMATION: NAME	CITY	STATE	ZIP CODE	COUNTRY
Crawford; Christopher M.	Washington	DC	20016	

APPL-NO: 08/ 813612 [PALM]
DATE FILED: March 10, 1997

PARENT-CASE:
This is a divisional application of application Ser. No. 08/145,825, filed Nov. 04, 1993 now U.S. Pat. No. 5,771,354, issued Jun. 23, 1998.

INT-CL: [06] H04 K 1/00

US-CL-ISSUED: 380/25; 380/49, 395/200.9, 395/200.15
US-CL-CURRENT: 705/34; 705/77, 709/217, 709/219, 709/238

FIELD-OF-SEARCH: 380/23, 380/25, 380/49, 380/4, 395/200.9, 395/200.15

PRIOR-ART-DISCLOSED:

U.S. PATENT DOCUMENTS

Search Selected | Search ALL

	PAT-NO	ISSUE-DATE	PATENTEE-NAME	US-CL
☐	4649479	March 1987	Advani et al.	
☐	4901223	February 1990	Rhyne	
☐	4954945	September 1990	Inoue et al.	
☐	4982234	January 1991	McConaughy et al.	
☐	4994963	February 1991	Rorden et al.	
☐	5023774	June 1991	Schuur	
☐	5089958	February 1992	Horton	
☐	5109515	April 1992	Laggis et al.	
☐	5210866	May 1993	Milligan et al.	
☐	5276867	January 1994	Kenley et al.	
☐	5317728	May 1994	Tevis et al.	
☐	5353411	October 1994	Nakaosa et al.	
☐	5404527	April 1995	Irwin et al.	
☐	5426594	June 1995	Wright et al.	
☐	5497479	March 1996	Hornbuckle	
☐	5515502	May 1996	Wood	
☐	5544320	August 1996	Konrad	395/200.09
☐	5696901	December 1997	Konrad	395/200.09

ART-UNIT: 276

PRIMARY-EXAMINER: Cain; David C

ATTY-AGENT-FIRM: Nixon & Vanderhye P.C.

ABSTRACT:

A user can use his personal computer to call up an on-line service system over a telecommunications link such as a telephone line. The On-line system provides all sorts of useful services to the personal computer such as antiviral protection, auxiliary processing capabilities, and other features that are impractical or inconvenient to provide locally.

173 Claims, 68 Drawing figures

End of Result Set

Generate Collection | Print

L4: Entry 2 of 2 File: USPT May 4, 1999

DOCUMENT-IDENTIFIER: US 5901228 A
TITLE: Commercial online backup service that provides transparent extended storage to remote customers over telecommunications links

Application Filing Date (1):
19970310

Brief Summary Text (8):
Because computer users often demand instantaneous sharing of computer information and cannot wait for someone to send them a floppy disk containing the information, various "on-line" personal computer connections have become popular. The computer user can connect a "modem" (a kind of data transmitter and receiver) between his computer and his telephone line. The computer controls the modem to automatically call the telephone number of another computer, which also has a similar modem connected between it and the telephone line. The two computers can "talk" to one another over the telephone line, and can exchange all sorts of information such as files, Email, and computer programs.

Brief Summary Text (16):
One problem with the Internet is that a local computer can directly access the resources of another computer, thus allowing a local computer to introduce a boot sector virus, for instance, on the system disk of a remote computer such that the remote computer will become infected the next time the remote computer is booted. NFS and RFS do utilize security controls to set the discretionary (public access as set by user) and mandatory (secured access defined through system maintained security attributes for each object on the system) controls when making a local file system available to the network. A remote user with proper authorities, however, still has direct access to the remote system's storage, however, and so the opportunity exists to transport unwanted data and programs to the remote system. This problem has cause serious consequences in the past (e.g., in 1988 a WORM virus spread throughout the Internet and infected many computers). "Local area networks" (LANS) are another common way to interconnect computers. Many businesses now store most or all of their important data on a special shared personal computer called a "file server." User computers access the shared file server over a high-speed data network called a "local area network" (LAN) or a "wide area network" (WAN). Briefly, a "local area network" interconnects data equipment within a limited geographical area, allowing user computers to communicate with each other and to share central resources such as printers, data storage, and long distance data communications. LANs are typically interconnected with coaxial copper cable, unshielded twisted pair cable, or fiber optics. Using a LAN to inter-connect computers provides a more efficient and faster means for data transfer than traditional file transfer methods. All users on a LAN can share resources such as printers, storage devices, and telecommunication links to limit costs associated with duplication of data and equipment. A LAN can also improve business functions with interconnected workstations accessing electronic mail and various shared applications such as customer service inquiry.

Brief Summary Text (20):
IBM also introduced a "Virtual Disk" function as part of its "PC Support." This function allows users to access personal computer programs and information by accessing the mini computer as if it were a locally-attached personal computer disk drive. Thus, the minicomputer simulates a local disk drive with a "virtual" or "simulated" disk that actually comprises hardware and software resources of the mid-range computer. In other words, the mid-range computer when attached to the

personal computer "looks like" a local disk drive to the personal computer. The personal computer "thinks" it is writing to a locally attached disk drive when actually its data is going through a communications (e.g., telephone) line and gets stored in the memory and/or hard disk of the minicomputer.

Brief Summary Text (24):
In one configuration, the IBM AS/400 can be used with dial-up telephone lines to attach "virtual disks" to remotely located personal computers. Modems are used to provide an interface between the AS/400 and standard dial-up telephone lines. The modems connect to a "communications controller" interface board within the AS/400. This "communications controller" board translates the data streams between the modem and the AS/400. Using these techniques, it is possible to have a remote personal computer call up the AS/400 over a dial up telephone line and attach to a "virtual disk" provided by the AS/400 (this requires both the remote personal computer and the AS/400 to run appropriate "PC Support" software). The personal computer assigns a drive designator (e.g., "E") to the "virtual disk." If the computer user commands the personal computer to write to the "C" drive, the personal computer will write the information to the local PC hard disk. If the computer user, on the other hand, commands the personal computer to write to the "E" (virtual) disk drive, the personal computer "thinks" it is writing to a locally attached "E" disk but is instead sending its data over the telephone line for storage in the AS/400. Reading from the "E" drive retrieves files from the AS/400. The reader is referred to the IBM documentation concerning this function, and in particular, the "PC Support" manuals relating to the IBM System/36, System/38 and AS/400. See also IBM manuals relating to TCP/IP for the IBM RISC 6000 describing the "mount" command supported under the AIX operating system.

Brief Summary Text (72):
User authorization to access the host may be granted by a "sign-up" system. The "sign-up" system may create a configuration file including password and other access information, and download the file to the user's workstation. Initial charges may be collected via a user-supplied credit card number. Alternatively, access to the "sign-up" system may be via a "special pay" telephone number (900) such that compensation is received by the service provider from the user via the telephone company billing system.

Brief Summary Text (74):
A dialing pattern sent to a customer computer (e.g., a certain number of calls, certain number of rings each call, a certain wait period between each call) triggers the customer computer modem to switch into answer mode. Upon answer, an access code is optionally sent to the customer's computer that identifies a reason for the host call (i.e., dial back verification, host task completed on behalf of customer, mail or data waiting for download to customer, etc.). The host computer flags a customer record indicating the customer computer answered at the appropriate time (dialing pattern match), thereby allowing the customer computer to access the host. A Customer Signal file is used to queue the dial-up requests. This allows the host to trigger the customer to call the host when needed, and also allows the customer to be certain that only his computer can access the service. When the customer calls the service first, the service hangs up and queues a dialing pattern to be sent to the customer. Only when the customer computer answers after a certain dialing pattern will the host computer allow the customer entry. The customer accesses the service, but only after the host flags a dialing pattern match. If the host dials the customer first and gets a pattern match, then the customer can access the system immediately without this dialback sequence.

Detailed Description Text (10):
These and other problems and difficulties are eliminated when customer computer 50 connects to an on-line service system 100 provided by the preferred embodiment of the present invention via a data link 150 as shown in FIG. 1. Data link 150 may comprise a dial up telephone line or other similarly convenient telecommunications link that allows customer computer 50 to be located remotely to the on-line service system 100. The on-line service system 100 provides various capabilities (e.g., data storage, program storage, processing, and input/output devices) that enhance the operations of customer computer 50 in order to solve the drawbacks and problems mentioned above. On-line service system 100 provides software and computing services to customer computer 50 in return for fees. Such software and services can be extremely valuable to the user of customer computer 50 in that they provide enhancements to the operation of the customer computer that were available either not at all or only through great expense and/or inconvenience.

Detailed Description Te[redacted] (28):
In the preferred embodiment, replica computer 160 is capable of operating in an on-line mode or in an off-line mode. In the on-line mode, the replica computer 160 communicates interactively with customer computer 50 to perform processing tasks. In this on-line mode in the preferred embodiment, the customer computer 50 and the on-line replica computer 160 cooperate to support processing in either and/or both processors (shared access to data buffers and a record locking scheme is used to ensure safe access). In the off-line mode, replica computer 160 performs personal computer tasks in response to direction from host computer 104 without having an on-line, interactive link with customer computer 50.

Detailed Description Text (36):
Host computer 104 provides "virtual disk drives" to customer computer 50 and replica computer(s) 160 in the preferred embodiment through use of conventional software available from IBM. In the preferred embodiment, host computer 104 comprises an IBM AS/400 mid-range computer providing "PC Support" virtual disk, print and other associated functions. As explained above, the IBM-provided PC Support Software makes it easy to attach a "virtual disk" or virtual printer to a remote or local personal computer such as customer computer 50. For DOS machines, "PC Support" requires that certain device drivers (EIMPCS.SYS and ECYDDX.SYS) are resident in the memory of the customer computer 50 or replica computer 160 t provide memory management and PC to AS/400 routing support (of course, this technique can be used with other operating systems such as OS/2, Unix, etc. using appropriate virtual device and workstation software). These device drivers are loaded from the PC CONFIG.SYS file during the PC IPL process. Other programs are loaded during host session initiation to provide workstation and virtual device access. Different "shared folder" types (0, 1 and 2) provide different performance based on different overhead requirements (e.g., personal computer memory usage). The AS/400 allows a personal computer to attach to a "shared folder" as a "Folder Drive" this allows the PC user to assign a drive letter to a specific folder, or as a "System Drive" (this allows the PC user to assign a drive letter to all the folders the user is authorized to access). Using this method, the DOS Change Director (CD) command can be used to change from one virtual disk drive to another, and normal operating system commands can be used to access and manipulate the virtual disks.

Detailed Description Text (58):
FIG. 5 provides an overview of an example of the virtual disk drive attachment capabilities of the on-line service system 100. Two physical disk drives 116a, 116b are shown connected to the host computer 104. The host computer 104 is shown as a customer disk repository with host system disks 116a, 116b logically divided into customer virtual disks. Host computer physical disk drive 116a stores information associated with two different virtual disks (I:Drive and J:Drive), and host computer physical disk drive 116b stores information associated with a further virtual disk (K:Drive). The host computer 104 is shown with a communication link to the replica server computer 160 and a customer computer 50a. Two columns of drives shown within customer computer 50a identify the devices addressable by the customer processor. The first column, "Local Disk Drives," identifies the physical drives 64AA-64AC physically attached to the customer computer 50a. The second column, "Virtual Disk Drives," identifies the disk drives 136(1)-136(3) created from logically divided host storage (this may be the same or different storage is used to create virtual disk drives 136I-136K).

Detailed Description Text (59):
Three columns of drives shown within the replica computer 160 identify the devices addressable by the replica computer. The first column, "Local Disk Drives," identifies the drives 164A-164C physically attached to the replica computer (A:Drive, B:Drive, C:Drive). The second column, "Customer Disk Drives," identifies the disk drives 64BD-64BF physically attached to the customer computer 50 that have been redirected to the replica computer 160 as remote virtual disks (D:Drive, E:Drive, F:Drive) (these may be the customer computer A:Drive, B:Drive, C:Drive)). The third column, "Virtual Disk Drives," identifies disk drives 136I-136K created from logically divided storage of host computer 104. Although each column shows three drives, this is not meant to limit the number of attachable devices. The replica computer 160 is shown with a communication link 166 to the host computer and another communication link 150b to a customer computer.

Detailed Description Text (78):
FIG. 6E schematically shows some of the more important high level tasks performed by

each of the main components within the preferred embodiment (i.e., customer computer 50, host computer 100, and replica computer 160). Each of these tasks are performed under software control, and certain of these tasks may communicate with other tasks being performed by other computers. The customer computer 50 in the preferred embodiment supports the high-level functions of communications, logging, security, routing, program execution, local disk access, and remote disk access. The on-line service host computer 104 supports communications, logging, security, command control, program execution, host disk access and virtual disk access. The on-line and off-line replica computers 160 in the preferred embodiment each support communications, logging, security, routing, program execution, local disk access, and remote disk access. Each of the computers 50, 104 and 160 is provided with local physical mass storage disk. Thus, customer computer 50 has its local hard disk 64, host computer 104 has its local hard disk 116, and replica computer 160 has its local hard disk 164.

Detailed Description Text (101):
If the request is for "backup, restore and archive" services, host computer 104 logs certain information (e.g., user, begin time, etc.) for billing and security purposes (block 414), and then allocates ("mounts") the appropriate virtual disks containing the software needed to satisfy the request (block 416). The process of copying the information is performed in the preferred embodiment by customer computer 50 and/or replica computer 160 by copying information to and/or from a virtual disk (block 418). The end time is preferably then logged by host computer 104 for billing purposes (block 414).

Detailed Description Text (103):
If the request is for program or data rental (block 428), the appropriate information is logged as before (block 430), and the virtual disk storing the program or data to be rented is then allocated to the appropriate computer (e.g., customer computer 50 and/or replica computer 160) (block 432). A "host" security program is executed by the host computer 104 to prevent unauthorized copying of the virtual disk contents, and a similar program executes in the customer computer 50 and replica computer 160 to prevent unauthorized access to virtual disk data and programs residing in random access memory. The customer computer 50 and/or replica computer 160 executes the rental program or accesses the data (block 434). Meanwhile, host computer 104 keeps track of beginning and ending times of access to ensure that the customer can be billed based on the amount of time he has used the contents of the virtual disk (block 430). A customer can also be billed on a per use basis or a monthly charge basis.

Detailed Description Text (104):
In the preferred embodiment, the user may request to "purchase" a particular program or data. For example, the user may want his own copy of the program or data locally stored or he may wish to modify it such that it is not feasible to merely rent it. If the request is for a "purchase," logging is performed as before (block 438), and then the host computer 104 allocates the appropriate virtual disk containing the program or information to be purchased (block 440). Host computer 104 also allocates a destination device for receiving the purchased program or information (block 442). This destination device may be, for example, the local hard disk 64 within customer computer 50. The selected software is then copied to the destination device in order to complete the purchase (block 444). This copying operation is preferably performed only upon receipt of payment from the customer (e.g., by checking credit card authorization and charging the associated license fee to the customer's credit card account). Software demonstrations of the programs not requiring secured customer data can be made available to all customers by providing access to a shared, execute-only virtual disk. Demos allowing secured customer data can be provided by copying programs or information stored on a secured virtual disk to a temporary virtual disk with customer execute-only access. If payment is not received within a specified period, the virtual disk can be deleted. Upon receipt of payment, the temporary virtual disk ownership can be transferred to the customer for complete access. This enables the customer to obtain immediate access to the desired software while allowing the service provider to later revoke access if payment is not received.

Detailed Description Text (105):
If the request is for release update services (block 446), the request is logged as before (block 448), and host computer 104 also determines whether the customer is entitled to release update and also whether this particular customer wants or needs the release update (block 450). Assuming that the customer is authorized to receive,

wants and needs the upd[redacted]e, host computer 104 allocates a virtual disk storing the release update (more th[redacted] one may be transferred at the [redacted]e time) (block 452), and then copies and/or applies the updates to customer computer 50 (block 454). When necessary, a program can be executed to perform special services such as configuration changes to customer computer 50.

Detailed Description Text (106):
Blocks 456-462 provide a generic description of additional user request handling. Beginning and ending times are logged for billing and security (block 458), appropriate virtual disks and/or other virtual devices are allocated to handle the request (block 460), and appropriate software is executed and data is accessed within host computer 104 and/or replica computer 160 and/or customer computer 50 to handle the request (block 462).

Detailed Description Text (211):
FIG. 15 is a flowchart of program control steps performed by customer computer 50 to execute the "security check" routine shown in FIGS. 14A-14H. The purpose of the security check is to ensure that only "authorized" tasks are performed. The routine first obtains the command (block 742) and determines whether it was generated locally or by the remote computer (i.e., from the host 104 or the on-line replica 160). If the command is remotely originating (e.g., by a user of the replica computer 160 or by the host 104 via a "PC Execution" command; "no" exit to block 744), then block 746 screens the command to determine whether it is allowed. If the command is allowed, appropriate information is typically logged at the host computer 104 or the replica computer 160 system virtual disk for billing. If the command is not allowed, a security violation is logged at the customer server router 518 (block 750), a flag is set to tell the customer server router 518 to deny the request (block 752) and a violation message is sent to the controlling session (block 754).

Detailed Description Text (212):
If the command was entered by the user of the customer computer 50, it will generally be performed since the user should not be limited in what he can do with his own local computing resources and security checks performed at host 104 and replica computer 160 prevent the customer computer command from creating unauthorized accesses on those computers. There is an important exception, however, in the case of software rental. In instances in which the system 100 attaches a virtual disk to the customer computer 50 containing software that the user of customer computer 50 is only allowed temporary access to, the user could attempt to bypass the resource security to the virtual disk through various techniques. Resource security, which is used by the preferred embodiment AS/400 host 104 to control access to all of its stored "objects," can be used to control access to information within different "virtual drives" provided by the AS/400 host computer 104 to customer computer 50. For each object, resource security can be used to maintain specific or public authority. Specific authority describes the authority of individual users. Public authority describes the authority for all users who do not have specific authority. Resource security applies to each virtual disk drive, and to each object within the drive. The AS/400 supports the following file sharing modes when sharing files:

Detailed Description Text (218):
Note that the AS/400 security measures do not provide any "execute only" access to objects stored on a virtual disk. Thus, to grant execution rights to customer computer 50 over a particular program stored on a virtual disk, the preferred embodiment host 104 must allow the user authority to read the file. Read authority, in turn, grants a full right to copy the file. This "read" authority could thus be used by an unscrupulous user of customer computer 50 to take a copy of a rental program on a virtual disk without paying the appropriate license fee.

Detailed Description Text (224):
FIG. 18 is a flowchart of exemplary program control steps performed by the host computer 104 as part of the host security program 906. The first step performed is to read requests from the router (block 918). The "router" is a host program used to route personal computer virtual device accesses. The host security program 906 is a user exit program specified under network configuration and is called automatically by the router to validate requests. Decision block 920 then tests whether the customer has requested access to a secured device. In the preferred embodiment, all access to virtual devices during an on-line session are validated for security (this is in addition to user ID and object resource security). When a customer is running applications within her own customer computer 50 and a request to the host is issued

to change to a differen[redacted]on-line server virtual device" drive or subdirectory, the request is validated fo[redacted]access rights by decision block[redacted]0. Routine 906 then determines whether or not the request for a particular program and/or information is going to be allowed (block 922). This test is important for program rental and other secured access, in which case the router requests are validated to restrict programs and requests while attached to certain (virtual device) drives and subdirectories in the preferred embodiment. If access is allowed, then host computer 104 logs billing data, CPU time, storage type and usage to permit billing and audit trails (block 924). If the security check performed by block 922 fails, then host computer 104 logs the security violations (block 926), flags the router to deny access to the requested device (block 928), and sends a violation message to the controlling session (block 930).

Detailed Description Text (294):
Referring now to FIG. 19B, once it is decided by host computer 104 that a particular customer computer 50 will be signalled, the host computer logs signal and time for billing (block 952), allocates the modem 102 (block 954), and sends a dialing pattern to the telephone number of the customer computer having the appropriate number of calls, rings per call, and wait intervals between rings based upon the stored calling pattern within the customer control data block field 1002H (block 956). Host computer 104 next determines whether the customer computer answered (decision block 958). If not, host computer logs an error and gives up (block 960). If the host computer 104 detects that the customer computer 50 did answer, the host computer tests whether the customer computer answered on the appropriate ring of the final call (decision block 962). If the host computer 104 expected the customer computer 50 to answer on the fifth ring and it instead answered on the second ring, for example, host computer 104 will log an error and hang up (block 964). Errors within about one ring are ignored by the host computer because it is not possible to detect which ring an answering telephone goes off hook on with closer than an accuracy of about .+-.1 ring. This testing to ensure that the customer computer 50 picks up on the correct ring provides added authentication and security, since it allows the host computer 104 to have some assurance that it has contacted the appropriate customer computer 50.

Detailed Description Text (295):
If the signal customer data block 1000 specifies an access code in field 1000D (as tested for by decision block 966), then host computer 104 sends the appropriate access code (block 968), after the access code is sent (or if no access code is required), host computer 104 hangs up the modem 102 (block 970), and then may set a "sign-on allowed" flag (block 972) within customer control data dialback field 1002R (see FIG. 22B). In the preferred embodiment, when a signal is successfully sent, the customer computer 50 can access the system directly. When the dialback option is configured, a customer cannot access the system unless the system successfully sends a signal to the customer computer. This signal is sent when the customer first accesses the system, or if time triggered signal data is processed based upon a host or replica request. Host computer 104 then logs a "signal successful" message for billing and security purposes (block 974), and clears the signal data block 1000 associated with that particular signal.

Detailed Description Text (297):
Referring to FIG. 20A, host computer 104 reads the next host request from the host request file 1004 shown in FIG. 22C (block 978). If the conditions specified by the "start date/day and time" field 1004B of the host request file 1004 record are met (decision block 980), then host computer 104 reads the customer control data block 1002 associated with the particular customer computer to whom the request pertains (block 982). Host computer 104 then determines whether the customer computer 50 is currently logged on (decision block 984). In the preferred embodiment, the customer's on-line session task also reads host request data. Thus, if the customer is in an on-line session, the request will be managed by the on-line session rather than by the host request task 912.

Detailed Description Text (298):
Assuming that the host request task 912 is going to perform the request, host computer 104 determines whether an on-line session is necessary to satisfy the request (decision block 986). Some requests (e.g., requests for pure processing) can be satisfied without the associated customer computer 50 being logged on. Most other requests, however, require some input from or output to the customer computer 50 via a live, real-time on-line session. If an on-line session is required to perform a host request, signal data is written to a signal customer data block 1000, and the

host request is re-queued until the customer computer begins an on-line service session (blocks 988, 990, 992).

Detailed Description Text (321):
FIGS. 21A-21E together are a flowchart of exemplary program control steps performed by host computer 104 in order to begin an on-line session with a customer computer 50. Referring to FIG. 21A, host computer 104 validates user ID and password provided by the logged-on customer computer 50 (block 1102) and logs the sign-on information for billing and security purposes (block 1104). Host computer 104 then accesses the basic information associated with the customer computer 50 from the customer control data block 1002 associated with the user ID/password (block 1106). Host computer 104 checks within the customer control data block 1002 to determine whether the dialback option 1002R requires the host computer 104 to signal the customer computer 50 before allowing process requests (block 1108). If dialback is required, then host computer 104 checks the "sign-on allowed" flag of record 1002R to determine whether the "signal customer" task block 972 (FIG. 19B) set this flag properly to allow the customer computer 50 to call in. If the flag is not set, then the host computer 104 treats the call-in from the customer computer 50 as a request for the host computer to contact it, and writes a signal customer data block 1000 to that effect (block 1112). Host computer 104 then logs sign-off information for billing and security (block 1114), signs off the customer computer (block 1116), and disconnects (block 1118). Subsequently, as described previously in connection with the "signal customer" task of FIGS. 19A-19B, the host computer will contact the customer computer 50 in a more secure way. At this point, the host computer 104 refuses the customer computer contact because user ID and password security is deemed insufficient in the preferred embodiment to provide adequate security for the data being transferred via the on-line service.

Detailed Description Text (323):
Host computer 104 next queries its communications controller 112 to determine whether the customer computer is calling in on a special charge telephone number (e.g., a 900 number) (decision block 1126). If it is, host computer 104 displays a message specifying the service charges and prompts for acceptance within a specified time (block 1128). This gives the customer the opportunity to exit before phone charges begin. Basic charge amounts are also displayed. If the customer does not accept within a specified time (decision block 1130), host computer logs sign-off information for billing and security (block 1132), signs off the customer computer 50 (block 1134), and disconnects (block 1136). If the customer does accept, then host computer 104 sets a Telco billing access flag 1002W within the customer control data block 1002 to indicate that billing is being handled by the telephone company instead of by the host computer 104 (block 1138).

Detailed Description Text (324):
Referring now to FIG. 21C, host computer 104 attaches to customer computer 50, a virtual disk containing anti-viral software and forces the customer computer to execute the anti-viral code (blocks 1140, 1142). Host computer 104 then reads the host request file 1004 to see if there are any host requests outstanding for the particular customer (block 1144). If there are requests ("yes" exit to decision block 1146), host computer logs the request in time for billing (block 1148), and then logs information about pending requests until the requests are completed (block 1150). Host computer 104 then determines whether the request is for an off-line replica processing (block 1152). If it is not, then the host computer begins processing the request during the on-line session (block 1154) and, once it is completed, clears the host request (block 1156). If, on the other hand, the request is for an off-line replica computer 160 ("yes" exit to decision block 1152), host computer 104 prompts the user for associated parameters and copies the customer based data to a virtual device available to the replica computer 160 (blocks 1158, 1160). Host computer 104 then logs the request and end time for billing purposes (block 1162), and clears the host request (block 1164).

Detailed Description Text (325):
Referring now to FIG. 21D, assuming that things are going to proceed in an on-line session, host computer 104 displays request options to the customer computer 50 (block 1166). This allows the customer to select request options after or between host requests in the preferred embodiment. If the customer or a host request at any time issues a sign-off request (decision block 1168), host computer 104 logs the sign-off information for billing and security (block 1170), signs off the customer computer (block 1172) and disconnects (block 1174).

Detailed Description Text (326):
If the customer computer 50 or replica computer 60 issues a request (block 1176), host computer 104 logs the billing and pending table with request and begin time (block 1178). Host computer 104 then checks whether the request is for an off-line replica computer (block 1180). If it is not, then the host computer performs the request during the on-line session (block 1182). If the request is for an off-line replica, on the other hand ("yes" exit to decision block 1180), host computer 104 prompts for parameters and copies the customer based information to a virtual device for attachment to the replica computer (blocks 1184, 1186), and then logs the request and end time for billing (block 1188).

Detailed Description Text (327):
FIG. 21E is a flowchart of exemplary program control steps performed by block 1154 of FIG. 21C and block 1182 of FIG. 21D in order to process an on-line request, and block 1488 of FIG. 21F in order to process an off-line request. Host computer 104 first determines the authority of the host command to access restricted system objects (block 1190). In the preferred embodiment, customers are restricted from most system areas. The command used to perform a customer's request allows access to only the necessary areas of host computer 104. The host computer adopts the user authority to access customer objects (block 1192), and then determines the source and destination of the customer and host based data and software (block 1194). Host computer 104 then attaches whatever virtual devices (e.g., disks, printers, etc.) are needed for data and software (block 1196), and executes the requested task in the customer computer 50, replica computer 160 or host processor 106. Where the task is executed is based on the processor flag within the request, and is determined by the type of software to be executed (e.g., mini-computer or micro-computer) as well as other factors. In this context, the host command is capable of issuing a router command to execute the program in the customer's computer 50 when necessary. In the case of replica server sessions host commands routed to the workstation are first directed to the replica computer and replica server routing causes execution to occur in either the replica or customer computer (with or without command line translation) based on the processor flag in the customer control data. Blocks 1190-1198 are performed repeatedly until all commands have been executed (decision block 1200; a "command" may actually consist of many commands or a sequence of commands). Once the request has been completed ("yes" exit to decision block 1200), host computer 104 detaches the virtual devices that were attached at block 1196 (block 1202), and sends a completion message to the controlling session (block 1204). Host computer 104 then clears customer control data pending request table entry 1002N (see FIG. 22B), logs the customer control data completion message table entry 1002O (see FIG. 22B), and logs request and ending time for billing purposes (blocks 1206, 1208, 1210).

Detailed Description Text (334):
The command authority refers to the option during command creation that allows the command to adopt the authority of the commands owner during execution. The user profile of the owner of the command may be set up to have authority to host commands that the customer does not have on her own. The command authority is the authority of the secondary command processor call from FIG. 21E block 1198 (which typically would not provide authority to most system virtual disks). In the case of virtual disks used for system functions or owned by another customer, the allocation would be denied based on lack of user resource authority. In the case of virtual disks used to supply rental and purchase programs and info to customers, the allocation may be denied if it is determined the allocation should be limited to selection by menu or command option requested by the workstation programs described in FIGS. 21A and 21E (calling a CL command, FIG. 21E, with command authority (adopted from the owner of the command) to cause the allocation to be performed during execution within block 1198). In this situation, the customer would need to select the device allocation by host menu or command option (as previously described) before selecting the option to invoke a secondary command processor. In the case of public virtual disks or virtual disks with customer access authority, the allocation will be permitted for the authority requested (read/write) if host security allows for the user profile.

Detailed Description Text (336):
FIG. 21F is a flowchart of exemplary program control steps performed by the host computer 104 to manage an off-line replica session. The replica computer 160 first provides a user ID and associated password to establish authority to manipulate special customer objects (e.g., route virtual devices, etc.) (block 1480, 1482). The host computer 104 limits the authority of the replica computer 160 based on this

user ID. The off-line replica computer then reads the replica request file associated with it (see FIG. 25B), reads associated customer control data block 1002, and then redirects interrupts to manage automated keystrokes based upon a customer stored script (blocks 1484-1486). Various methods are available and well known for providing automated input for tasks. Basically, certain conditions and values such as data in the video buffer is identified after which data is moved into the keyboard buffer in response (including carriage return and other control characters). This leaves the impression of an interactive session with the customer. The replica computer then logs the request in time for billing purposes (block 1487), and begins processing the request (block 1488) by executing appropriate software. Once the request is completed, the replica computer 160 writes a "completion message" to the host request file (block 1489), and routes data if necessary to a different customer using route data replica request (block 1491). Block 1491 asks if the request includes routing results to another customer. If so, host computer 104 writes a "route data" replica request and signal data request for the different customer to receive these results to the replica request data file (block 1493); and finally, writes a signal customer data for the "route data" destination user (block 1495).

Detailed Description Text (337):
A significant difference between the on-line workstation programs represented by FIGS. 21A and 21F is that FIG. 21A (on-line replica computer 160) receives all command and menu option input either interactively by the customer or by requests read from the Host Request file, whereas the workstation program represented by FIG. 21F (off-line replica computer) receives all command and menu option input from requests read from the Replica Request file (off-line requests). The workstation program in FIG. 21F also issues PC execution commands within the off-line replica to reconfigure interrupts to satisfy input requests with script data provided by the Off-line Replica Request. This redirection involves chaining interrupt handlers used to test for various conditions (video buffer content, timeout, etc.) and provide input based on a match test. Common between the workstation programs described in FIGS. 21A and 21F is that both satisfy on-line service requests (some of which are described in FIG. 22H "Request Options") by calling CL programs generically described by FIG. 21F "Begin Process Request" block 1488. Each of the request options are satisfied by a separate CL program following the general functionality of FIG. 21E. That is to say, the CL commands are created with the authority of the owner of the command to access resources the customer may not have under her own user profile. The CL command adopts customer or replica user ID authorities to access customer objects. Virtual devices are allocated to satisfy the request. Execution is performed in the appropriate processor. Virtual devices are detached and the command is logged.

Detailed Description Text (353):
In the preferred embodiment, host computer 104 maintains billing records in the form of a billing data log 1008 shown in FIG. 22F. This billing data block contains the following information useful for billing purposes:

Current US Original Classification (1):
705/34

End of Result Set

Generate Collection | Print

L6: Entry 1 of 1 File: USPT May 4, 1999

DOCUMENT-IDENTIFIER: US 5901228 A
TITLE: Commercial online backup service that provides transparent extended storage to remote customers over telecommunications links

US Patent No. (1):
5901228

Brief Summary Text (8):
Because computer users often demand instantaneous sharing of computer information and cannot wait for someone to send them a floppy disk containing the information, various "on-line" personal computer connections have become popular. The computer user can connect a "modem" (a kind of data transmitter and receiver) between his computer and his telephone line. The computer controls the modem to automatically call the telephone number of another computer, which also has a similar modem connected between it and the telephone line. The two computers can "talk" to one another over the telephone line, and can exchange all sorts of information such as files, Email, and computer programs.

Brief Summary Text (20):
IBM also introduced a "Virtual Disk" function as part of its "PC Support." This function allows users to access personal computer programs and information by accessing the mini computer as if it were a locally-attached personal computer disk drive. Thus, the minicomputer simulates a local disk drive with a "virtual" or "simulated" disk that actually comprises hardware and software resources of the mid-range computer. In other words, the mid-range computer when attached to the personal computer "looks like" a local disk drive to the personal computer. The personal computer "thinks" it is writing to a locally attached disk drive when actually its data is going through a communications (e.g., telephone) line and gets stored in the memory and/or hard disk of the minicomputer.

Brief Summary Text (24):
In one configuration, the IBM AS/400 can be used with dial-up telephone lines to attach "virtual disks" to remotely located personal computers. Modems are used to provide an interface between the AS/400 and standard dial-up telephone lines. The modems connect to a "communications controller" interface board within the AS/400. This "communications controller" board translates the data streams between the modem and the AS/400. Using these techniques, it is possible to have a remote personal computer call up the AS/400 over a dial up telephone line and attach to a "virtual disk" provided by the AS/400 (this requires both the remote personal computer and the AS/400 to run appropriate "PC Support" software). The personal computer assigns a drive designator (e.g., "E") to the "virtual disk." If the computer user commands the personal computer to write to the "C" drive, the personal computer will write the information to the local PC hard disk. If the computer user, on the other hand, commands the personal computer to write to the "E" (virtual) disk drive, the personal computer "thinks" it is writing to a locally attached "E" disk but is instead sending its data over the telephone line for storage in the AS/400. Reading from the "E" drive retrieves files from the AS/400. The reader is referred to the IBM documentation concerning this function, and in particular, the "PC Support" manuals relating to the IBM System/36, System/38 and AS/400. See also IBM manuals relating to TCP/IP for the IBM RISC 6000 describing the "mount" command supported under the AIX operating system.

Detailed Description Text (10):
These and other problems and difficulties are eliminated when customer computer 50

connects to an on-line service system 100 provided by the preferred embodiment of the present invention via a data link 150 as shown in FIG. 1. Data link 150 may comprise a dial up telephone line or other similarly convenient telecommunications link that allows customer computer 50 to be located remotely to the on-line service system 100. The on-line service system 100 provides various capabilities (e.g., data storage, program storage, processing, and input/output devices) that enhance the operations of customer computer 50 in order to solve the drawbacks and problems mentioned above. On-line service system 100 provides software and computing services to customer computer 50 in return for fees. Such software and services can be extremely valuable to the user of customer computer 50 in that they provide enhancements to the operation of the customer computer that were available either not at all or only through great expense and/or inconvenience.

Detailed Description Text (294):
Referring now to FIG. 19B, once it is decided by host computer 104 that a particular customer computer 50 will be signalled, the host computer logs signal and time for billing (block 952), allocates the modem 102 (block 954), and sends a dialing pattern to the telephone number of the customer computer having the appropriate number of calls, rings per call, and wait intervals between rings based upon the stored calling pattern within the customer control data block field 1002H (block 956). Host computer 104 next determines whether the customer computer answered (decision block 958). If not, host computer logs an error and gives up (block 960). If the host computer 104 detects that the customer computer 50 did answer, the host computer tests whether the customer computer answered on the appropriate ring of the final call (decision block 962). If the host computer 104 expected the customer computer 50 to answer on the fifth ring and it instead answered on the second ring, for example, host computer 104 will log an error and hang up (block 964). Errors within about one ring are ignored by the host computer because it is not possible to detect which ring an answering telephone goes off hook on with closer than an accuracy of about .+-.1 ring. This testing to ensure that the customer computer 50 picks up on the correct ring provides added authentication and security, since it allows the host computer 104 to have some assurance that it has contacted the appropriate customer computer 50.

Detailed Description Text (323):
Host computer 104 next queries its communications controller 112 to determine whether the customer computer is calling in on a special charge telephone number (e.g., a 900 number) (decision block 1126). If it is, host computer 104 displays a message specifying the service charges and prompts for acceptance within a specified time (block 1128). This gives the customer the opportunity to exit before phone charges begin. Basic charge amounts are also displayed. If the customer does not accept within a specified time (decision block 1130), host computer logs sign-off information for billing and security (block 1132), signs off the customer computer 50 (block 1134), and disconnects (block 1136). If the customer does accept, then host computer 104 sets a Telco billing access flag 1002W within the customer control data block 1002 to indicate that billing is being handled by the telephone company instead of by the host computer 104 (block 1138).

10/024734

WEST Search History

DATE: Friday, July 18, 2003

Set Name side by side	Query	Hit Count	Set Name result set
	DB=USPT; THES=ASSIGNEE; PLUR=YES; OP=OR		
L18	L17 and l7	1	L18
L17	L16 and l3	11	L17
L16	(connect$ with (host or differen$) with network$) and @ad<=19980116	10548	L16
L15	3648243.pn. and (log$ same (access$ with (time or duration)))	1	L15
L14	5910987.pn. and (log$ same (access$ with (time or duration)))	1	L14
L13	5930772.pn. and (log$ same (access$ with (time or duration)))	1	L13
L12	5956697.pn. and (log$ same (access$ with (time or duration)))	1	L12
L11	5970477.pn. and (log$ same (access$ with (time or duration)))	1	L11
L10	6073108.pn. and (log$ same (access$ with (time or duration)))	1	L10
L9	6349289.pn. and (log$ same (access$ with (time or duration)))	1	L9
L8	6349289.pn.	1	L8
L7	L6 and (log$ same (access$ with (time or duration)))	7	L7
L6	L5 and log$	28	L6
L5	L3 and l2	33	L5
L4	L3 andl2	379	L4
L3	((705/30 |705/32)!.CCLS.)	379	L3
L2	L1 and (bill$ or charg$ or cost$)	10021	L2
L1	((access$ with (time or duration)) same (authentic$ or author$ or permit$ or allow$)) and @ad<=19980116	17517	L1

END OF SEARCH HISTORY

End of Result Set

Generate Collection | Print

L9: Entry 1 of 1 File: USPT Feb 19, 2002

US-PAT-NO: 6349289
DOCUMENT-IDENTIFIER: US 6349289 B1

TITLE: Method and system for tracking computer system usage through a remote access security device

DATE-ISSUED: February 19, 2002

INVENTOR-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY
Peterson; Bruce Lee	Crystal Lake	IL		
Clayton; Christina Ellen	Chicago	IL		
Farmer; Michael Stephan	Wildwood	MO		

ASSIGNEE-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY	TYPE CODE
Ameritech Corporation	Hoffman Estates	IL			02

APPL-NO: 09/ 008344 [PALM]
DATE FILED: January 16, 1998

INT-CL: [07] G06 F 17/60

US-CL-ISSUED: 705/34; 705/26, 705/30, 705/40, 709/227
US-CL-CURRENT: 705/34; 705/26, 705/30, 705/40, 709/227

FIELD-OF-SEARCH: 705/34, 705/26, 705/27, 705/30, 705/40, 358/400, 379/114.1, 379/112.1, 709/227

PRIOR-ART-DISCLOSED:

U.S. PATENT DOCUMENTS

Search Selected | Search ALL

	PAT-NO	ISSUE-DATE	PATENTEE-NAME	US-CL
☐	3798605	March 1974	Feistel	
☐	4672572	June 1987	Alsberg	
☐	4800590	January 1989	Vaughan	
☐	4944007	July 1990	Austin	
☐	5003584	March 1991	Benyacar et al.	
☐	5068894	November 1991	Hoppe	
☐	5113499	May 1992	Ankney et al.	
☐	5115466	May 1992	Presttum	
☐	5120939	June 1992	Claus et al.	
☐	5196840	March 1993	Leith et al.	
☐	5216703	June 1993	Ray	
☐	5276444	January 1994	McNair	
☐	5291551	March 1994	Conn et al.	
☐	5317636	May 1994	Vizcaino	
☐	5361062	November 1994	Weiss et al.	
☐	5392345	February 1995	Otto	
☐	5412723	May 1995	Canetti et al.	
☐	5481613	January 1996	Ford et al.	
☐	5534857	July 1996	Laing et al.	
☐	5535276	July 1996	Ganesan	
☐	5546379	August 1996	Thaweethai et al.	370/254
☐	5553239	September 1996	Heath et al.	
☐	5560008	September 1996	Johnson et al.	
☐	5586260	December 1996	Hu	
☐	5606617	February 1997	Brands	
☐	5661807	August 1997	Guski et al.	
☐	5740361	April 1998	Brown	713/201
☐	5778071	July 1998	Caputo et al.	713/159
☐	5790548	August 1998	Sistanizadeh et al.	370/401
☐	5862203	January 1999	Wulkan et al.	379/114
☐	5867494	February 1999	Krishnaswamy et al.	
☐	5867495	February 1999	Elliott et al.	370/352
☐	5887065	March 1999	Audebert	
☐	5893077	April 1999	Griffin	705/34
☐	5907610	May 1999	Onweller	379/242

FOREIGN PATENT DOCUMENTS

FOREIGN-PAT-NO	PUBN-DATE	COUNTRY	US-CL
558326	September 1993	EP	
2271696	April 1996	GB	
05118861	May 1993	JP	
WO 8302343	July 1983	WO	
WO 9946691	September 1999	WO	

OTHER PUBLICATIONS

Hewlett-Packard, Accounting System Planning and Billing, Aug., 1992, 1-4.

ART-UNIT: 2765

PRIMARY-EXAMINER: Nguyen; Cuong H.

ATTY-AGENT-FIRM: Brinks Hofer Gilson & Lione

ABSTRACT:

A system and method for monitoring remote computer access and associated costs is provided. The system includes a remotely located communication server in communication with multiple host computer networks and in communication with a network access server. First and second memory devices contain a list of authorized users for the host computer networks and a user log for use by a billing computer to generate bills. The method includes the steps of creating starting and ending time stamps for each authorized user accessing a respective one of the multiple host computer networks and creating a user log to generate bills and monitor host computer network usage.

13 Claims, 2 Drawing figures

End of Result Set

Generate Collection | Print

L9: Entry 1 of 1 File: USPT Feb 19, 2002

DOCUMENT-IDENTIFIER: US 6349289 B1
TITLE: Method and system for tracking computer system usage through a remote access security device

Abstract Text (1):
A system and method for monitoring remote computer access and associated costs is provided. The system includes a remotely located communication server in communication with multiple host computer networks and in communication with a network access server. First and second memory devices contain a list of authorized users for the host computer networks and a user log for use by a billing computer to generate bills. The method includes the steps of creating starting and ending time stamps for each authorized user accessing a respective one of the multiple host computer networks and creating a user log to generate bills and monitor host computer network usage.

US Patent No. (1):
6349289

Detailed Description Text (10):
The pass code preferably consists of a fixed personal identification number and a time variable security token. The security token may be a soft token, such as a software application on each authorized user's computer, or a hard token, such as a secure ID card 14 available from Security Dynamics, Inc. Each authorized user preferably has her own security token and the security token may be a sequence of numbers, letters, or other type of symbol. Using the secure ID card 14, the security token is obtained by the user from a display that generates a new security token at predetermined time increments. The NAS 30, containing an identical security token generating algorithm synchronized with the secure ID card 14 generates the same security token to verify that the user is an authorized user. On authentication, the communication server 20 connects the user computer 12 to the appropriate host computer 34 for the duration of the call. The NAS 30 receives an ending time stamp from the communication server 20 at the conclusion of the remote access call when the user hangs up or otherwise disconnects from the host computer network 34 (at step 54). Following the conclusion of the remote access call, the service bureau stores the starting and ending time stamps in the NAS memory. Preferably the starting and ending time stamps are associated in the user log with the list of authorized users so that the user log contains a record of computer time usage for each authorized user (at step 56).

Detailed Description Text (16):
From the above, a new system and method of monitoring access and fees for host computer networks with relocated users is provided. The method includes maintaining a list of host computer networks and associated list of authorized users for each network, creating a starting and ending time stamp for remote access calls, transmitting the starting and ending time stamps in the user log to a billing computer in addition to other billing information, and generating a billing summary of costs and usage at the billing computer. The system preferably includes a security service bureau providing secure remote access between remotely located authorized users and their respective proprietary host networks. In one preferred embodiment, the NAS preferably records time stamps and a user log indicating usage of resources by individual authorized users. A billing computer is also included in the system having the logic necessary to compile information from the user log in the security service bureau and cost information received from outside sources to generate a periodic bill indicating cost per individual user and/or department.

CLAIMS:

1. In a system for providing secure remote access between a plurality of unrelated host computer networks and a plurality of authorized users via a network access server, a method of monitoring access to each of the unrelated host computer networks comprising the steps of:

maintaining a list of host computer networks and an associated list of authorized users for each host computer network in a first memory device;

automatically creating a starting time stamp at the beginning of a remote access call received from an authorized user at a communication server and connecting the authorized user to an appropriate one of the plurality of unrelated host computer networks after determining at the network access server that the authorized user is authorized to connect to the appropriate one of the plurality of unrelated host computer networks;

automatically creating an ending time stamp at a conclusion of the remote access call;

storing the starting and ending time stamps for the remote access call in a user log in the network access server, the starting and ending time stamps associated with the list of authorized users whereby the user log contains a record of computer time usage for each authorized user;

transmitting the user log from the network access server to a billing computer;

transmitting the list of host computer networks and the associated list of authorized users for each host computer network from the first memory device to the billing computer; and

generating a billing summary at the billing computer for each of the host computer networks.

12. In a system for providing secure remote access between a plurality of unrelated host computer networks and a plurality of authorized users via a network access server, a method of monitoring access to each of the unrelated host computer networks comprising the steps of:

maintaining a list of host computer networks and an associated list of authorized users for each host computer network in a first memory device;

receiving a remote access telephone call to a host computer network from a user computer of an authorized user at a communication server;

automatically creating a starting time stamp at the beginning of the remote access call received from an authorized user at the communication server and connecting the authorized user to an appropriate one of the plurality of unrelated host computer networks after determining at the network access server that the authorized user is authorized to connect to the appropriate one of the plurality of unrelated host computer networks;

automatically creating an ending time stamp when the user computer terminates the remote access call with the host computer;

storing the starting and ending time stamps for the remote access call in a user log in the network access server, the starting and ending time stamps associated with the list of authorized users whereby the user log contains a record of computer time usage for each authorized user;

transmitting the user log from the network access server to a billing computer;

transmitting the list of host computer networks and the associated list of authorized users for each host computer network from the first memory device to the billing computer; and

generating a billing summary at the billing computer for each of the host computer networks.

End of Result Set

Generate Collection | Print

L10: Entry 1 of 1 File: USPT Jun 6, 2000

US-PAT-NO: 6073108
DOCUMENT-IDENTIFIER: US 6073108 A

TITLE: Task-based classification and analysis system

DATE-ISSUED: June 6, 2000

INVENTOR-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY
Peterson; Andrew C.	Long Beach	CA		

ASSIGNEE-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY	TYPE CODE
Paul, Hastings, Janofsky & Walker	Los Angeles	CA			02

APPL-NO: 08/ 668579 [PALM]
DATE FILED: June 21, 1996

INT-CL: [07] G06 F 17/60

US-CL-ISSUED: 705/8; 705/7, 705/9, 705/30, 705/34
US-CL-CURRENT: 705/8; 705/30, 705/34, 705/7, 705/9

FIELD-OF-SEARCH: 705/8, 705/9, 705/7, 705/30, 705/34

PRIOR-ART-DISCLOSED:

U.S. PATENT DOCUMENTS

Search Selected | Search ALL

	PAT-NO	ISSUE-DATE	PATENTEE-NAME	US-CL
☐	5077666	December 1991	Brimm et al.	705/2
☐	5175681	December 1992	Iwai et al.	705/9
☐	5182705	January 1993	Barr et al.	705/11
☐	5189608	February 1993	Lyons et al.	705/30
☐	5311423	May 1994	Clark	705/8
☐	5325290	June 1994	Cauffman et al.	705/34
☐	5329447	July 1994	Leedom, Jr.	705/9
☐	5343387	August 1994	Honma et al.	705/9
☐	5530861	June 1996	Diamant et al.	705/8
☐	5566333	October 1996	Olson et al.	707/102
☐	5991742	November 1999	Tran	705/41

OTHER PUBLICATIONS

Heck, Mike. "Primavera's Sure Trak Answers Midsize Scheduling Needs," InfoWorld, vol. 17, No. 15, pp. 71-3, Apr. 10, 1995.
England, Cheryl. "Taking Care of Business," MacUser, vol. 11, No. 4, pp. 92-99, Apr. 1995.
J. Mallory, "Software for Windows captures billable time," Newsbytes, Jun. 20, 1994.

"Timeslips 5." Law Office Technology Review, vol. 2, No. 5-1, May 7, 1992.
"A junior partner to manage your workflow," Law Office Technology Review, vol. 3, No. 4, Apr. 29, 1994.
"A lawyer's PIM plus," Law Office Technology Review, vol. 4, No. 4, Apr. 6, 1995.
"Case management with Abascus Law +,"Law Office Technology Review, vol. 4, No. 92, Sep. 25, 1995.
"PCLAWjr to automate the small law firm," Law Office Technology Review, vol. 2, No. 3-3, Mar. 24, 1992.

ART-UNIT: 272

PRIMARY-EXAMINER: Stamber; Eric W.

ASSISTANT-EXAMINER: Rhodes; Jason W.

ATTY-AGENT-FIRM: Oppenheimer Wolff & Donnelly LLP

ABSTRACT:

A task-based classification and analysis system includes an analysis software module and a user interface. The analysis software module establishes and maintains relationships between a plurality of databases or, in a preferred embodiment, hierarchical task lists. The user interface provides user inputs to the analysis software module such as budget information which is associated with particular elements of the databases. In consideration of historical data models, the user inputs and predetermined relationships between elements of the databases, the preferred system generates information products such as task-based budgets. Another preferred system coordinates task relationships between a plurality of software modules, such as a billing software module and a time entry software module.

16 Claims, 12 Drawing figures

End of Result Set

Generate Collection | Print

L10: Entry 1 of 1 File: USPT Jun 6, 2000

DOCUMENT-IDENTIFIER: US 6073108 A
TITLE: Task-based classification and analysis system

US Patent No. (1):
6073108

Brief Summary Text (5):
U.S. Pat. No. 5,182,705 to Barr et al. discloses a computer system and method for work management. Staff Tables are used to maintain authority levels for access to certain functions such as billing, docketing, etc. The disclosed system also includes an Activity Log used to track billing. Accessed information such as a description of the work done and the time spent are then directly fed into an automatic billing function. Additionally, a Local Data function facilitates the customization of data recordation and output at a local level.

End of Result Set

Generate Collection | Print

L11: Entry 1 of 1 File: USPT Oct 19, 1999

US-PAT-NO: 5970477
DOCUMENT-IDENTIFIER: US 5970477 A

TITLE: Method and system for allocating costs in a distributed computing network

DATE-ISSUED: October 19, 1999

INVENTOR-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY
Roden; Barbara J.	Atlanta	GA		

ASSIGNEE-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY	TYPE CODE
BellSouth Intellectual Property Management Corporation	Atlanta	GA			02

APPL-NO: 08/ 679965 [PALM]
DATE FILED: July 15, 1996

INT-CL: [06] G06 F 7/00

US-CL-ISSUED: 705/32; 709/218, 709/229, 709/219, 379/112, 379/127, 380/4
US-CL-CURRENT: 705/32; 379/112.01, 705/78, 709/218, 709/219, 709/229

FIELD-OF-SEARCH: 705/32, 364/514, 395/200.59-59

PRIOR-ART-DISCLOSED:

U.S. PATENT DOCUMENTS

Search Selected | Search ALL

	PAT-NO	ISSUE-DATE	PATENTEE-NAME	US-CL
☐	5717604	February 1998	Wiggins	364/514
☐	5737414	April 1998	Walker et al.	380/4
☐	5745556	April 1998	Ronen	379/127
☐	5778182	July 1998	Cathey et al.	395/200.49
☐	5815665	September 1998	Teper et al.	395/200.59
☐	5864604	January 1999	Moen et al.	379/112
☐	5870550	February 1999	Wesinger, Jr. et al.	395/200.48

FOREIGN PATENT DOCUMENTS

FOREIGN-PAT-NO	PUBN-DATE	COUNTRY	US-CL
0192071 A2	August 1986	EP	
0765068 A2	March 1997	EP	
19535378 A1	March 1997	DE	
WO 95/23483	August 1995	WO	
WO 95/33236	December 1995	WO	
WO 96/37848	November 1996	WO	
WO 97/01920	January 1997	WO	
WO 97/29584	August 1997	WO	

ART-UNIT: 275

PRIMARY-EXAMINER: MacDonald; Allen R.

ASSISTANT-EXAMINER: Patel; Jagdish

ATTY-AGENT-FIRM: Jones & Askew, LLP

ABSTRACT:

A method and system for providing an end-user with Internet access and allocating a cost associated with that access among the end-user and Internet sites 18 accessed by the end-user. A supervisory program module 58, such as a "JAVA" applet, resides on an originating station 24, such as a personal computer, operated by the end-user. The supervisory program module 58 may be activated by transmitting the supervisory program module to the originating station 24 from an Internet point of presence 22 operated by a local access provider. Alternatively, a trigger may be transmitted from the point of presence 22 to the originating station 24 to activate a supervisory program module 58 already residing on the originating station 24. The supervisory program module 58 monitors the duration of connections with specific Internet sites, and transmits messages to the point of presence 22 indicating the duration of these connections. The local access provider uses the information received in these messages to allocate a cost associated with the access, such as the cost associated with using a telephone network 30, among the end-user and Internet sites accessed by the end-user. Unique keys and time stamps are used as security measures. Unique keys are random identification numbers or codes generated by the point of presence 22. Time stamps are clock readings are generated by the originating station, the point of presence, or other network components, are used as security measures.

27 Claims, 6 Drawing figures

End of Result Set

Generate Collection | Print

L11: Entry 1 of 1 File: USPT Oct 19, 1999

DOCUMENT-IDENTIFIER: US 5970477 A
TITLE: Method and system for allocating costs in a distributed computing network

US Patent No. (1):
5970477

Drawing Description Text (6):
FIG. 5 is a logic flow diagram illustrating a method for providing an end-user with Internet access and monitoring the duration of connection between an end-user and an Internet site in accordance with the preferred embodiment of the present invention.

Detailed Description Text (32):
The supervisory program module 58 monitors Internet activity conducted by the end-user station 24 and transmits messages to the credit server 42. More specifically, the supervisory program module 58 monitors the end-user's access to an Internet site 18 in the free zone by transmitting a "start.sub.-- free" message to the credit server 42 when the end-user station 24 transmits a URL request for the Internet site 18. The supervisory program module 58 later transmits a "stop.sub.-- free" message upon the occurrence of a predefined event, typically transmission of a URL request for another Internet site. These start.sub.-- free and stop.sub.-- free messages each include "time stamps" or clock readings generated by the supervisory program module 58 based on the clock 51 controlled by the end-user station 24, along with the IP address and user name associated with the end-user station 24 and the URL or IP address of the accessed Internet site 18. The credit server 42 stores the contents of the start.sub.-- free and stop.sub.-- free messages in the credit log 44 to provide a record of the end-user's connect time with the Internet site 18. When the credit log 44 is downloaded to the billing system 46, the end-user's connect time with the Internet site 18 is computed as the difference between the time stamp of the stop.sub.-- free message less the time stamp of the start.sub.-- free message.

Detailed Description Text (47):
FIG. 5 is a logic flow diagram illustrating a method for providing an end-user with Internet access and monitoring the duration of connection between an end-user and an Internet site. The logic flow diagram of FIG. 5 further describes routine 414 shown on FIG. 4. The process illustrated by FIG. 5 is terminated when the communication between the end-user station 24 and the point of presence 22 is disconnected, indicated by the "YES" branch from step 416 of FIG. 4. It should be understood that the communication may be disconnected at any time during the operation of the routine illustrated by FIG. 5.

End of Result Set

Generate Collection | Print

L12: Entry 1 of 1 File: USPT Sep 21, 1999

US-PAT-NO: 5956697
DOCUMENT-IDENTIFIER: US 5956697 A

TITLE: Timer-based fee-charging system for internet

DATE-ISSUED: September 21, 1999

INVENTOR-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY
Usui; Tatsuo	Tokyo			JP

ASSIGNEE-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY	TYPE CODE
International Scientific Co., Ltd.	Tokyo			JP	03

APPL-NO: 08/ 701493 [PALM]
DATE FILED: August 22, 1996

FOREIGN-APPL-PRIORITY-DATA:

COUNTRY	APPL-NO	APPL-DATE
JP	8-201166	July 11, 1996

INT-CL: [06] G06 F 17/00

US-CL-ISSUED: 705/32; 705/44, 345/326, 395/200.33, 395/200.47
US-CL-CURRENT: 705/32; 345/741, 705/44, 709/203, 709/217

FIELD-OF-SEARCH: 705/32, 705/18, 705/44, 345/326, 345/335, 395/200.33, 395/200.47, 395/200.49

PRIOR-ART-DISCLOSED:

U.S. PATENT DOCUMENTS

Search Selected | Search ALL

	PAT-NO	ISSUE-DATE	PATENTEE-NAME	US-CL
☐	5749075	May 1998	Toader et al.	705/14

ART-UNIT: 274

PRIMARY-EXAMINER: Peeso; Thomas R.

ATTY-AGENT-FIRM: Dilworth & Barrese

ABSTRACT:

A timer-based fee-charging system for Internet services eliminates the inconveniences of contracting which are necessary with Internet providers as well as payments of usage fees and subscription rights, etc., and allows instant access to Internet connection services through an easy access and payment method. Such a system consists of: a terminal server to provide Internet access to clients; an authentication server to confirm whether or not a client is gaining access based on specific information input by the client; an extended authentication database, linked to the authentication server, which controls authentication data comprising specific information of, and the access status rate that indicates a predetermined available time range for access for, each client; a fee-charging server, linked with the extended authentication database, which constantly renews the access status rate by calculating access charges according to the amount of access time each client uses.

18 Claims, 2 Drawing figures

End of Result Set

Generate Collection | Print

L12: Entry 1 of 1 File: USPT Sep 21, 1999

DOCUMENT-IDENTIFIER: US 5956697 A
TITLE: Timer-based fee-charging system for internet

US Patent No. (1):
5956697

Brief Summary Text (11):
The present invention is composed of a terminal server--which can provide connections to the Internet for many and unspecified clients, and an extended authentication data base, which can precisely manage the maximum amount of authentication data. This data consists of specific (personal) information--such as a unique log-in name and password--which responds to each client, and authentication data which consists of the access status rate, to indicate a predetermined available time for use. This is programmed in advance, in relation to the specific personal information, as above. The authentication server interlocks with a specific extended authentication data base to check access status to the Internet, according to a command from a specific terminal server, based on the specific information input(ted) by the client. The fee-charging server is interlocked with the specific extended authentication data base which calculates the fee for access according to the length of the time each client is connected, and constantly renews the access status rate of each authentication data of a specific extended authentication data base.

Detailed Description Text (24):
2. In case a client has logged in already, and the present time is more than the fee time, the access fee is calculated from the access time and is to be charged from the access status rate of the authentication data according to the access status rate for each time. If the specified access status rate falls below zero, the port resets, and the connection is cut.

Detailed Description Text (25):
Also, for the sake of connecting to the Internet, the connecting information input by a client is controlled by printing it on a card for each authentication data, so that it can be connected by the act of inputting specific information with a keyboard. Or the information can be controlled by being recorded on a card with magnetic codes for each authentication card, and it is also possible to have it connected by inserting the specific card into a recorder which is connected with a personal computer. At that time, the items of information which are to be printed (on a card in the former case), include access status rate number, support URL, domain name, domain name server IP-address, POP server name, log-in name, password, and so on.

End of Result Set

Generate Collection | Print

L13: Entry 1 of 1 File: USPT Jul 27, 1999

US-PAT-NO: 5930772
DOCUMENT-IDENTIFIER: US 5930772 A

TITLE: Volume-dependent accounting system and method in connectionless communications

DATE-ISSUED: July 27, 1999

INVENTOR-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY
Gomyo; Hisayuki	Tokyo			JP
Horiguchi; Hiroshi	Tokyo			JP
Hattori; Junichi	Tokyo			JP
Kato; Hiroaki	Tokyo			JP
Fujiwara; Kentaro	Tokyo			JP

ASSIGNEE-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY	TYPE CODE
Fujitsu Limited	Kawasaki			JP	03

APPL-NO: 08/ 777660 [PALM]
DATE FILED: December 31, 1996

FOREIGN-APPL-PRIORITY-DATA:

COUNTRY	APPL-NO	APPL-DATE
JP	8-076295	March 29, 1996

INT-CL: [06] G06 F 17/00

US-CL-ISSUED: 705/30; 705/18, 707/9, 707/10
US-CL-CURRENT: 705/30; 705/18, 707/10, 707/9

FIELD-OF-SEARCH: 705/18, 705/30, 707/1, 707/9, 707/10, 707/102, 707/205, 395/200.33, 395/200.47, 395/200.49, 395/200.61

PRIOR-ART-DISCLOSED:

U.S. PATENT DOCUMENTS

Search Selected | Search ALL

	PAT-NO	ISSUE-DATE	PATENTEE-NAME	US-CL
☐	5608874	March 1997	Ogawa et al.	395/200.15

ART-UNIT: 274

PRIMARY-EXAMINER: Peeso; Thomas R.

ATTY-AGENT-FIRM: Staas & Halsey

ABSTRACT:

When an accounting process is performed through connectionless communications such as a WWW, etc., a retrieval CGI stores a retrieval result in a file having a file name generated from a process ID and a user ID. Then, a retrieving/accounting process is performed in units of a user ID and a process ID. A session is managed using the process ID as information to be exchanged, thereby requiring no resident combinational software. Furthermore, a volume-dependent accounting can be realized even when communications are disconnected.

25 Claims, 14 Drawing figures

End of Result Set

Generate Collection | Print

L13: Entry 1 of 1 File: USPT Jul 27, 1999

DOCUMENT-IDENTIFIER: US 5930772 A
TITLE: Volume-dependent accounting system and method in connectionless communications

US Patent No. (1):
5930772

Brief Summary Text (14):
A basic volume-dependent system is based on the time of access obtained from the access log of the server. However, communications are often disconnected on the network, and the user may not be able to obtain the transmitted contents. Therefore, correctly recording an "access" into the log does not indicate that the requested information has been successfully transmitted to the user.

Detailed Description Text (22):
(5) A system should be designed to serve a large number of users. In this case, user access includes plural times of access using the same user identifier (including a double log-in, etc).

Detailed Description Text (64):
If the retrieval result is accessed a first time, the accounting process 27 is requested to perform an accounting process. The accounting process 27 records an accounting log in the accounting log file 28.

Detailed Description Text (71):
In FIG. 10, processes P3 and P4 are the same as those shown in FIG. 3. In this example, access is gained a first time to the retrieval result file, and an accounting log is generated by the accounting process 27. If the retrieval result cannot be successfully transmitted, the browser is kept in a retrieval result wait state without displaying any data on the screen, or in a state where the retrieval result is displayed halfway.